U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the DOI PIA Guide for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project: Microsoft Office 365 Cloud
Bureau/Office: Office of the Chief Information Officer
Date: August 3, 2020
Point of Contact
Name: Teri Barnett
Title: Departmental Privacy Officer
Email: DOI_Privacy@ios.doi.gov
Phone: (202) 208-1605
Address: 1849 C Street NW, Room 7112, Washington, DC 20240

Section 1. General System Information

A. Is a full PIA required?

☒ Yes, information is collected from or maintained on
- ☐ Members of the general public
- ☐ Federal personnel and/or Federal contractors
- ☐ Volunteers

☒ All

☐ No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

The Department of the Interior (DOI) has an enterprise agreement for Microsoft Office 365 Multi-Tenant & Supporting Services including Azure Active Directory (O365), which is a cloud service product of Microsoft that enables common Enterprise Architecture through a flexible and convenient cloud offering. Bundling of Office 365 services allows DOI to simplify administration of licenses and subscriptions to services at an enterprise level, and facilitates system-wide user management, password administration, and oversight of security controls. The O365 services replaced the Google applications. Information was migrated from BisonConnect-Google Apps for Government to O365 BisonConnect.

This privacy impact assessment (PIA) evaluates privacy implications for DOI's use of the cloud-based O365 service products within O365 BisonConnect which are listed below. This PIA will be updated to address any additional privacy risk as other service products are implemented. The primary O365 applications currently available Department-wide by default include:

- O365 BisonConnect Outlook will provide email and calendar capabilities to all the Department's employees, contractors and volunteers. For archival and discovery purposes, O365 BisonConnect mail will be captured and stored by DOI's email archiving and e-Discovery systems. The Default Global Address List provides directory listings for all users, distribution list, and resources of O365 BisonConnect system, in alphabetical order. Users may access this application on their government-furnished mobile devices.
- SharePoint Online provides online collaborative sites that are visible to personnel within the DOI domain and can be used to share any information, some of which may contain personally identifiable information (PII), in the form of reports, contact information, and others. SharePoint Online can help staff share information, organize projects and teams, and discover people and information. BisonConnect users have the option to create their own websites that will be visible on the DOI domain. Users have virtually unlimited options with respect to the types of pages created and the information included. Web pages may include text, PDFs, images, audio, or video files.
- OneDrive for Business (ODfB) is a cloud-based storage repository that facilitates creation, storage, sharing, and collaborative work for all types of electronic files which may include documents, forms, reports, correspondence, briefing papers, committee and meeting minutes, contracts, grants, leases, permits, audits, manuals, studies, promotional materials, compliance information and other confidential information. The files in ODfB are private by default and can only be viewed by the file creator. Files may be made searchable by the file creator, and by system administrators for authorized purposes such as eDiscovery. However, the users can alter permissions for their files in the drive, and the file rights can be further delineated to view only, view and comment, or view, comment, and edit. ODfB allows staff to share information with business colleagues as needed and edit Office documents together in real time with Office Online.   It can also sync files to a local computer using the ODfB sync application. Due to the nature of ODfB, users may store all types of electronic files including text, graphical, audio, or video files, which may include documents, forms, reports, correspondence, briefing papers, committee and meeting minutes, contracts, grants, leases, permits, audits, manuals, studies, promotional materials, compliance information, and other documents. There is a potential that large amounts of PII may be included in the documents stored in ODfB.

- MS Teams offers DOI users a calendar and centralized managed and stored instant messaging (IM) collaboration repository, including audio, video, and desktop sharing, and an extensive integration across O365 applications to assist DOI employees to create, organize, edit, comment on and share content of mutual interest. MS Teams allows users to record their team meetings capturing video, audio and screenshare activity. Data will be stored in MS Stream, a video service allowing DOI users to securely store and share their recordings. Users may access this application on their government-furnished mobile devices.
- Skype for Business Online (SfB) provides instant messaging (IM), audio and video calls, online meetings, availability (presence) information, and screen sharing capabilities within the Skype application. Skype for Business Online allows staff to connect with co-workers and leverages multiple devices to reach stakeholders through an enterprise-grade, secure, Information Technology (IT) managed platform. Contact information such as phone numbers and email addresses are used to communicate and connect users, which are only viewable by the specific user of the service. SfB is only used by these DOI Bureaus and Office; Bureau of Reclamation (BOR), Bureau of Land Management (BLM), and Office of the Special Trustee for American Indians (OST). This service will be used until July 2021 when Microsoft deprecates the service, at which time, BOR, BLM and OST will transition to MS Teams.
- Office Online is the web browser version of Word, PowerPoint, Excel, and OneNote. Office Online opens Word, Excel, OneNote, and PowerPoint documents in a web browser, and makes it easier to work and share Office files from any location with an Internet connection, from almost any device, and provides O365 customers with the capability to view, create, and edit files.
- Forms is a web-based application in O365 within SharePoint that allows users to create forms such as surveys, quizzes, and polls with internal users within the DOI environment. Forms sharing can be set to within DOI or for specifically invited guest users. Form creators are responsible for setting the appropriate access permissions for their forms. Forms permissions may be set to “Anyone with the link can respond” so responses are anonymous, and Forms will not record responders’ names unless the form owner turns that feature on to capture names, or Forms may be set to collect names and responses. Each form owner is responsible for ensuring that a Privacy Act Statement or Privacy Notice is provided on their forms as appropriate. Creators are responsible for ensuring their forms have being reviewed by their Information Collection Clearance Officer for specific requirements under the Paperwork Reduction Act and OMB Control numbers. Form owners are also responsible for working with their bureau APO to identify, assess, and manage privacy risks related to collection, use, and dissemination of PII information have been properly assessed, addressed and follow applicable Federal laws, Executive Orders, directives, policies, regulations, and standards.

Microsoft Office 365 Government features over forty productivity tools, use of these additional applications is reviewed by DOI’s Change Control Board process. These optional tools, such as MyAnalytics, help users manage their work activities and access authorized content for official use. The permissions for documents in these tools are the same as the primary applications. The tools use document permissions that are set by users on documents where they are stored in the primary applications, such as in ODfB or SharePoint Online. Individuals can only see documents in the tools that they have access to through sharing permissions in the primary applications. Permissions are not changed by these tools. Users are responsible for restricting the level of access to prevent others from accessing or downloading their files or folders. DOI bureaus/offices and employees may request the use of these add-ons or applications by contacting the DOI IT Helpdesk.

The DOI Office of the Chief Information Officer (OCIO) will provide management and oversight of Office 365, including system administration, security, enforcement of privileged users, authentication processes, and monitoring of the system. By default, the applications above are available enterprise-wide, however, individuals may request other applications within Microsoft Office 365 Government. Due to the nature of these applications, there may be a high degree of collaboration and data sharing at the local level. Storage and collaboration applications such as ODfB and SharePoint Online also allow users to upload data of their choice which could include documents and reports that contain PII. Each bureau, office or program utilizing these O365 applications is responsible for meeting the requirements of the Privacy Act of 1974, E-Government Act of 2002, and related privacy laws, policies and standards for the PII collected, used, maintained, or processed within their environment.

C. What is the legal authority?

5 U.S.C. 301, Departmental Regulations; 44 U.S.C. Chapter 35, the Paperwork Reduction Act; 40 U.S.C. 1401, the Clinger-Cohen Act; 44 U.S.C. 3541 et seq., Federal Information Security Modernization Act of 2014; OMB Circular A-130, Managing Information as a Strategic Resource; Executive Order 13571, “Streamlining Service Delivery and Improving Customer Service,” April 11, 2011; Presidential Memorandum, “Security Authorization of Information Systems in Cloud Computing Environments,” December 8, 2011; and Presidential Memorandum, “Building a 21st Century Digital Government,” May 23, 2012

D. Why is this PIA being completed or modified?

☐ New Information System
☐ New Electronic Collection
☐ Existing Information System under Periodic Review
☐ Merging of Systems
☒ Significantly Modified Information System
☐ Conversion from Paper to Electronic Records
☐ Retiring or Decommissioning a System
☐ Other: *Describe*

E. Is this information system registered in CSAM?

☒ Yes: *Enter the UII Code and the System Security Plan (SSP) Name*

UII Code: 010-000000330; Microsoft O365 Cloud System Security and Privacy Plan

☐ No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
None	None	No	N/A

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

☐ Yes: *List Privacy Act SORN Identifier(s)*
☒ No

Data extracts and sources are not directly collected by O365 BisonConnect system applications. PII contained in an email may be covered under a variety of existing DOI and government-wide systems of records. O365 BisonConnect does not create a new system of records.

H. Does this information system or electronic collection require an OMB Control Number?

☐ Yes: *Describe*
☒ No

Section 2. Summary of System Data

A. What PII will be collected? Indicate all that apply.

☒ Name
☒ Citizenship
☒ Gender
☒ Birth Date
☒ Group Affiliation
☒ Marital Status
☒ Biometrics
☒ Other Names Used
☒ Truncated SSN
☒ Legal Status
☒ Place of Birth
☒ Religious Preference
☒ Security Clearance
☒ Spouse Information
☒ Financial Information
☒ Medical Information
☒ Disability Information
☒ Credit Card Number
☒ Law Enforcement
☒ Education Information
☒ Emergency Contact
☒ Driver's License
☒ Social Security Number (SSN)
☒ Personal Cell Telephone Number
☒ Tribal or Other ID Number
☒ Personal Email Address
☒ Mother's Maiden Name
☒ Home Telephone Number
☒ Child or Dependent Information
☒ Employment Information
☒ Military Status/Service
☒ Mailing/Home Address
☒ Race/Ethnicity
☒ Other: *Specify the PII collected*

All these types of PII could potentially be included by users of these services. O365 contains username, work email address, work phone number, work address, title of DOI employee and contractor, and related organizational information required for system administration. Outlook provides a contact service that allows users to maintain contact information, including phone numbers and email addresses, which may include both work-related and personal contact information. This information is manually entered by the service user. Due to the nature of ODfB, users may store all types of electronic files including text, graphical, audio, or video files, which may include documents, forms, reports, correspondence, briefing papers, committee and meeting minutes, contracts, grants, leases, permits, audits, manuals, studies, promotional materials, compliance information, and other documents. There is a potential that large amounts of PII may be included in the documents stored in ODfB. Information about individuals may include, but is not limited to, names, email addresses, telephone numbers, Social Security numbers (SSNs), dates of birth, financial information, employment history, educational background, correspondence or comments from members of the public, and other information related to a specific mission purpose. Forms may collect various types of PII or information on user behaviors. Form owners are also responsible for working with their bureau APO to ensure appropriate authority for the collection, privacy notice is provided, and privacy risks are addressed.

B. What is the source for the PII collected? Indicate all that apply.

☒ Individual
☐ Federal agency
☐ Tribal agency
☐ Local agency
☒ DOI records
☐ Third party source
☐ State agency
☒ Other: *Describe*

Sources of information are system administrators and users of the services who create, add, store or upload information. Information was also migrated from BisonConnect-Google Apps for Government. Information added by O365 BisonConnect users about themselves. O365 BisonConnect users have a number of opportunities to voluntarily enter their own personal information, such as enhanced profile information, or personal information included in files added to OneDrive, personal images included in uploaded videos, or personal information included in blog posts or websites created by the user.

Information added by O365 BisonConnect users about other individuals. Users can also enter other users' PII into O365 BisonConnect in several ways, including entering enhanced contact information in the Contact database, uploading electronic files or videos that include other individual's personal information, or including personal information in documents, chats, or web pages in O365 BisonConnect. BisonConnect users will receive email from external email senders that includes PII, including information contained in the body and accompanying attachments.

C. How will the information be collected? Indicate all that apply.

☐ Paper Format
☒ Email
☐ Face-to-Face Contact
☒ Website
☐ Fax
☐ Telephone Interview
☒ Information Shared Between Systems *Describe*
☒ Other: *Describe*

DOI's employee Active Directory (AD) system, external sources, such as other Federal, Tribal, state, or local agencies, private third-party entities and members of the public who correspond with DOI bureaus, offices, programs or officials via the email system or otherwise provide data that is transmitted via the email system or entered into O365 BisonConnect applications. System administrators provide access to user groups at the bureau and office level. Each bureau or office has their own process and forms to request and provision user accounts authenticated by Enterprise AD. AD promulgates updates across the DOI domain, which will be used to enable authentication to the O365 applications. Storage and collaboration applications such as ODfB and SharePoint Online also allow users to upload data of their choice which could include documents and reports that contain PII. There is a potential that large amounts of PII may be included in the documents stored in ODfB. Users may store all types of electronic files including text, graphical, audio, or video files, which may include documents, forms, reports, correspondence, briefing papers, committee and meeting minutes, contracts, grants, leases, permits, audits, manuals, studies, promotional materials, compliance information, and other documents. Each bureau/office program utilizing these O365 services is responsible for ensuring proper use of O365 and for meeting privacy and security requirements within their organization.

O365 BisonConnect is integrated with the Symantec Vontu Data Loss Prevention (Symantec DLP) software. Symantec DLP monitors internet email and chat traffic to protect against the external transmission of sensitive data, including information concerning individuals such as SSNs. All O365 BisonConnect email and chat traffic crosses the Symantec DLP, but data is only retained when a security violation is detected. The data retained includes IP address, time of transmission and the transmitted data. Messages sent through Teams Chat can be edited but not deleted and may be considered Federal records and subject to the Freedom of Information Act.

Information about members of the public can be added to the system in a number of ways, including:

- Senders or recipients of email messages may be members of the public.

- Email messages may, in the subject, body or any attachments, include information about members of the public.
- O365 BisonConnect users may add contact information about members of the public to their contact databases.
- Electronic files added to OneDrive may include information about members of the public.
- Information added to SharePoint may include information about members of the public.
- Individuals may be invited as guest users in Teams.

D. What is the intended use of the PII collected?

PII is used to control access to the system by system administrators. Bureaus/offices also use work related PII to control access to the services. Information is collected from Bison Connect account holders who can be employees, contractors, or volunteers. This information is used to set-up the O365 BisonConnect email account. Users' valid DOI AD credentials are used to create O365 BisonConnect accounts. An O365 BisonConnect account cannot exist unless it corresponds to a valid AD account.

O365 services such as MS Teams or Skype for Business Online will allow users to view contact information to interact with each other within the collaborative environment. ODfB is used to store documents for collaborative interaction between individuals. SharePoint Online provides a storage and collaborative environment for DOI personnel and offices to interact with each other within DOI. PII may be used for a variety of purposes within the SharePoint, Forms, and ODfB components at the local level by specific programs in support of a specific mission purpose. Due to the purpose of the system and the range of supported services, personal information may be present in these tools for a variety of reasons as part of the function of program office during communication, collaboration, and creation and management of records.

E. With whom will the PII be shared, both within DOI and outside DOI? Indicate all that apply.

☒ Within the Bureau/Office: *Describe the bureau/office and how the data will be used.*

O365 BisonConnect may receive PII data on DOI employees in the form of email messages from DOI employees or contractors conducting official business through email correspondence or transfer of electronic files (file attachments). Correspondence will be conducted for official government purposes, which will vary depending on the mission and needs of the Bureau or Office.

Data is shared within the Office of Secretary to grant and manage access to the services and contents stored within ODfB and Sharepoint Online for collaboration purposes. System administrators have access to system data and system audit logs in order to manage access roles, monitor system usage, perform system audits, and complete other necessary job functions. Each user of the service will have access to their own data within the system and will be able to access other contents based on rights granted.

☒ Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*

O365 BisonConnect may receive PII data on DOI employees in the form of email messages from DOI employees or contractors conducting official business. This may be through email correspondence or transfer of electronic files (file attachments). Such correspondence will be conducted for official government purposes, which will vary depending on the mission and needs of the Bureau or Office.

Data is shared with bureaus and offices to grant and manage access to the services and contents stored within ODfB, MS Teams and SharePoint Online for collaboration purposes. System administrators have access to system data and audit logs in order to manage access roles, monitor system usage, perform system audits, and complete other necessary job functions. Each user of the service will have access to their own data within the system and will be able to access other contents based on rights granted.

☒ Other Federal Agencies: *Describe the federal agency and how the data will be used.*

Other Federal agencies do not have direct access to the system or any services within the system. However, data may be shared with other Federal agencies as necessary to meet legal or mission requirements, or in the course of conducting official business. For example, exchange of communications or correspondence generated from use of the services. Authorized sharing with external agencies will be made pursuant to DOI mission authorities and applicable system of records notices for each program area utilizing the services.

☒ Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*

Tribal, state or local agencies do not have direct access to the system or any services within the system. Data may be shared with other Tribal, state or local agencies as necessary to meet legal or mission requirements, or in the course of conducting official business.

☒ Contractor: *Describe the contractor and how the data will be used.*

Microsoft is a Cloud Service Provider (CSP) that will manage the environment. Per contractual obligations, they have no authorization to review, audit, transmit, or store DOI data. DOI may have contractor support within program areas, and these contractors will have limited access to contents of the services in the system.

☒ Other Third Party Sources: *Describe the third party source and how the data will be used.*

Third party organizations do not have direct access to the system or any services within the system. Data may be manually shared with other third parties as authorized and necessary to meet legal or mission requirements, or in the course of conducting official business.

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

☒ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

Each user voluntarily provides minimum information and consents to rules of behavior before being granted access to DOI computer network and resources. Requesting access and using the services are voluntary; however, the employee information is required to create and activate user accounts to access the services. Not providing information will prevent the user from accessing the DOI network and computing resources as DOI employees' username and contact information is provided by DOI employees for the essential purpose of user access control and account management within the DOI domain to fulfill their job duties in the course of business.

Individuals who are the subject of email communications or data within the O365 BisonConnect applications do not have the opportunity to consent to uses of information within the system but may have that opportunity at the time the data is collected or requested by a DOI bureau, office or employee. O365 BisonConnect users may be able to reduce the collection of information by reducing their use of O365 BisonConnect, including limiting email communication and file uploads. Users can also exercise discretion with respect to the PII they provide in O365 BisonConnect, including limiting PII in emails and email signature blocks.

☐ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

G. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☐ Privacy Act Statement: *Describe each applicable format.*

☒ Privacy Notice: *Describe each applicable format.*

Notice is provided to individuals through the publication of this privacy impact assessment.

☒ Other: *Describe each applicable format.*

All DOI employees with access to the DOI computer network, information and information systems are provided a login banner when logging on to the DOI network or Government Furnished Equipment (GFE) desktops/laptops to access O365 BisonConnect, and must acknowledge acceptance and understanding prior to being granted access to DOI computer resources. The login banner is not presented to GFE mobile phone users, however, prior to receiving their GFE phones and being granted access to DOI information systems and resources, users acknowledge and agree to DOI computer-network system monitoring.

☐ None

H. How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).

There are numerous ways data can be retrieved. ODfB and SharePoint Online have built-in searching capabilities which can be queried based on keyword, author, and other relevant information. Documents may be accessed through keyword search of any text or field contained in the document. MS Teams and Skype for Business Online utilizes a search capability to locate contact information based on name.

Mail: By default, messages are sent to each user’s inbox, and sorted by date and time of receipt. All replies are grouped with their original message, creating a single conversation or thread. Users have the option to create and sort inboxes using different folders, specific rules governing email handling, sorting and retrieval. Users can search for messages using one or more search criteria, including sender (partial or full name or email address of sender), email subject, full message text search, inclusion of an attachment, and date parameters.

Calendar: By default, calendar data is organized in chronological form using a traditional calendar view. The calendar can be adjusted to view day, week, month, four days, or agenda (which lists scheduled events in chronological order). Users can also perform a full text search of their calendar, including searching by name.

Documents stored in OneDrive can be accessed using the default “MyDrive” directory tree that lists the documents and folders in each user’s drive, as well as documents and folders owned by other users to which the user has been granted access. In addition, documents can be accessed through a keyword search feature that permits searches by name in the author field or throughout the text of the document.

Sites: Users can access O365 BisonConnect sites by performing keyword searches of BisonConnect sites, including searching by personal identifiers such as name.

I. Will reports be produced on individuals?

☒ Yes: *What will be the use of these reports? Who will have access to them?*

DOI produces a report on email collections when a court subpoenas email records of a O365 BisonConnect user. The data may include from, to, subject, date, and the contents of the email message.

☒ No

The system will not generate reports on individual O365 BisonConnect users. O365 BisonConnect’s auditing system allows reports to be generated on various aspects of the system's operating controls, including system functions and user actions; however, these reports provide only aggregated information and not information specific to individuals. O365 BisonConnect maintains an administrator dashboard that logs administrator access. The log contains administrator name and a list of administrative actions taken, such as records changes or activation or deactivation of system features.

Section 3. Attributes of System Data

A. How will data collected from sources other than DOI records be verified for accuracy?

O365 BisonConnect contains a set of tools that promote communication and collaboration. Due to the nature of the system and the anticipated broad use of these services across the enterprise, it is the responsibility of each user to ensure accuracy of data at the time the data is created, collected or used. System administrators ensure user information is accurate through user request form submitted by the users and through authentication with the AD service, and will not ensure accuracy of specific data created or entered by end users.

When a user's employment status is changed in AD, O365 BisonConnect administrators will remove the user's account from BisonConnect and the user's contact information will be purged from the Contacts database. These controls are outlined in the standard operating procedures for the BisonConnect System. Individuals submitting through forms are responsible for the accuracy of the data provided. The form or data owner is responsible for ensuring accuracy and meeting privacy requirements in accordance with the Privacy Act and Federal policy.

B. How will data be checked for completeness?

O365 BisonConnect contains a set of tools that promote communication and collaboration. Due to the nature of the system and the anticipated broad use of these services across the enterprise, it is the responsibility of each user to ensure completeness of data. SharePoint Online and ODfB data owners are responsible for verifying and updating the information relevant to the service to which they subscribe. Upon request from the users, the users' specific account attributes within Skype or MS Teams can be updated, which may be contact information. System administrators ensure completeness of user information for access control and authentication with the AD service, and will not ensure data created or entered by end users is complete.

C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).

O365 BisonConnect contains a set of tools that promote communication and collaboration. Due to the nature of the system and the anticipated broad use of these services, it is the responsibility of each user to ensure currency of the data created or used. System administrators will use processes to ensure user information is current and authenticated with the AD service, and will not ensure specific data created or entered by end users is current. AD is updated immediately upon a change in an employee's status, which will automatically update access to the system as only active and authorized employees will have access. When a user account is disabled or terminated, all access will be denied since the user will no longer have the ability to log onto or authenticate to the application. User contact information will be removed once the user account is deleted within the organization. Skype for Business Online allows user to add individual contact information or have the user contact information be generated from an organizational directory or group. Within the organization, users have the ability to enter their own information and to ensure that it is current.

D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.

Retention periods vary depending on the user created or manage contents and purpose of the program records. Records contained within ODfB and SharePoint Online are retained and disposed of in accordance with applicable Departmental and bureau/office records schedules, or General Records Schedule (GRS) approved by the National Archives and Records Administration (NARA) for each type of record based on the subject or function and records series.

System administration or AD records are maintained under the Departmental Records Schedule (DRS)-4.1, Short Term Information Technology Files, System Maintenance and Use Records (DAA-0048-2013-0001-0013), and System Planning, Design, and Documentation (DAA-0048-2013-0001-0014). These records include IT files that are necessary for day-to-day operations but not long-term justification of the bureau/office's activities. The disposition of these records is temporary. Records covered under DAA-0048-2013-0001-0013 have a temporary disposition and will be cut off when superseded or obsolete and destroyed no later than three years after cut-off. Records covered under DAA-0048-2013-0001-0014 have a temporary disposition and will be cut off when superseded by a newer version of upon termination of the system and destroyed three years after cut-off.

E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?

Procedures for disposition of the data stored in individual applications will vary by program office and needs of the agency. Due to the nature of Sharepoint Online and ODfB, there may be numerous records schedules with different dispositions applicable to the records created and maintained by users. It is the responsibility of each program office and user that creates or maintains Federal records to maintain and dispose of the records in accordance with the appropriate records schedule and disposition authority that covers their program area. Approved disposition methods include shredding or pulping for paper records, and degaussing or erasing for electronic records, in accordance with NARA Guidelines and 384 Departmental Manual 1.

F. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.

There is a moderate risk to the privacy of individuals for the use of O365 BisonConnect due to the nature of the services and the potentially significant amount of PII that may be contained in the system by users. O365 BisonConnect is a subscription service offering a shared pool of computing resources that may include a significant amount of PII. The level of risk associated with the type and sensitivity of PII is dependent on the bureau, office or program use and the safeguards implemented to mitigate the risk. Information stored within Skype for Business Online includes name, email address, work phone, work address, and title of DOI employees and contractors. The use of Forms, SharePoint Online and ODfB allows some PII such as personal phone number, home phone number to be entered and stored in the system, and may include other personal information such as the employee personal contact information, survey responses, and other information.

Due to the nature of ODfB, users may store all types of electronic files including text, graphical, audio, or video files, which may include documents, forms, reports, correspondence, briefing papers, committee and meeting minutes, contracts, grants, leases, permits, audits, manuals, studies, promotional materials, compliance information, and other documents. There is a potential that large amounts of PII may be included in the documents stored in ODfB. Information about individuals may include, but is not limited to, names, email addresses, telephone numbers, SSNs, dates of birth, financial information, employment history, educational background, correspondence or comments from members of the public, and other information related to a specific mission purpose. To mitigate the privacy risks, DOI has implemented a series of administrative, technical and physical controls.

The Department utilizes a combination of technical and operational controls to reduce risk in the O365 BisonConnect environment, such as firewalls, encryption, audit logs, least privileges, malware identification, and data loss prevention policies. All users must have a DOI account and government issued personal identity verification (PIV) card to access O365 BisonConnect. Bureaus and offices utilizing the O365 BisonConnect service are responsible for implementing adequate controls to safeguard PII used or maintained within their environment as appropriate. As part of the continuous monitoring program, continual auditing will occur on the system to identify and respond to potential impacts to PII information stored within the O365 environment, which will help the agency effectively maintain a good privacy and security posture for the system. The system privacy plan outlines the privacy controls and is reviewed annually to ensure adequacy of controls implemented to protect data.

Microsoft O365 is a FedRAMP approved cloud service provider and regularly undergoes reviews to ensure that all security controls are in place and operating as intended. O365 is rated as FISMA moderate based upon the type and sensitivity of data, and requires strict security and privacy controls to protect the confidentiality, integrity, and availability of the sensitive data contained in the system. Prior to granting users access to the DOI network, all users must agree to the DOI Rules of Behavior, as well as the DOI Warning Banner before access the system, which includes the consent to monitoring, and restrictions on data usage.

O365 BisonConnect is a cloud-based system that utilizes a private cloud community, as opposed to a public cloud service delivery model. Use of a private cloud significantly decreases penetration threats and associated risks. O365 BisonConnect uses a variety of operational and technical controls to restrict unauthorized access and use. In addition, O365 BisonConnect employs a variety of management, operational and technical security controls. Administrative access to O365 BisonConnect is granted only to authorized personnel on an official need-to-know basis. Unique administrator identification and authentication, passwords, least privileges and audit logs are utilized to ensure appropriate permissions and access levels. In addition, all administrative personnel, including contractors, must consent to rules of behavior and take annual end-user security awareness training, computer security role-based training, privacy awareness training, and role-based privacy training, and records training in order to obtain and maintain O365 BisonConnect administrator access.

There is a risk that individuals may be able to view files, or folders when access is mistakenly or unknowingly shared by the owner. Users of O365 must take proper precautions when setting access permissions to ensure only those with a need to know are granted access. O365 applications do not change access permissions on files and folders, access is controlled by the owner. For example, MyAnalytics does not allow anyone but the user to access their personalized information, unless that person purposefully and independently shares that information. Files created in ODfB or SharePointOnline and set to “People in DOI with the link” will be sharable and viewable by all O365 users.

There is a risk that authorized users will conduct unauthorized activities such as using, extracting and sharing information with unauthorized recipients. DOI’s user identity management processes include authentication with AD to control and manage access restrictions to authorized personnel on an official need-to-know basis. System administrators utilize user identification, passwords, least privileges, and audit logs to ensure appropriate permissions and access levels. The contract between DOI and O365 does not allow the service provider to review, audit, transmit, or store DOI data, which minimizes privacy risks from the vendor source. All DOI employees and contractors must complete privacy, security and records management awareness training, as well as role-based training where applicable, on an annual basis.

O365 BisonConnect can also operate on personally owned equipment (POE) that has been enrolled in the DOI secure POE containerization program. In this scenario, it is important to recognize that all personal data (personal emails, photos, etc.) maintained external to the container, including personally installed smart device applications, are not available to DOI and therefore cannot be inventoried, viewed or changed unless requested by legal action prompted by the U.S. government or authorized legal authorities. A special circumstance may exist when a user is working on an email that becomes part of a Freedom of Information Act, records or legal request. Although a remote possibility, data that exists in a draft form (e.g., unsent emails) may exist only within the container environment and may require the temporary collection of the POE. In these cases, discovery efforts will be limited to the container environment on the POE.

There is a risk that information may be maintained longer than necessary to accomplish a legitimate purpose or in accordance with an approved records retention schedule. This risk is mitigated by maintaining records in accordance with NARA approved records schedules. O365 BisonConnect records retention schedule is maintained under Departmental Records Schedule (DRS)-4.1, Short Term Information Technology Files, System Maintenance and Use Records (DAA-0048-2013-0001-0013), and System Planning, Design, and Documentation (DAA-0048-2013-0001-0014). Due to the nature of BisonConnect email, SharePoint Online and ODfB, there may be numerous records schedules with different dispositions applicable to the records created and maintained by users. It is the responsibility of each program office and user that creates or maintains Federal records to dispose of records in accordance with the appropriate records schedule and disposition authority that covers their program area. All personnel must complete records management training annually to ensure they understand records management responsibilities. Messages sent using Teams Chat can be edited but not deleted, and may be considered Federal records under the Federal Records Act, and subject to the Freedom of Information Act.

There is a risk of unauthorized collection, use and dissemination of PII using Microsoft Forms. Form owners are responsible for working with their bureau APO to identify, assess, and manage privacy risks related to collection, use, and dissemination of PII through Microsoft Forms have been properly assessed, addressed and follow applicable Federal laws, Executive Orders, directives, policies, regulations, and standards. Data loss prevention (DLP) policies are enabled in the Office 365 Security & Compliance Center to identify, monitor, and automatically protect sensitive information across Office 365.

There is a risk that non-DOI guests may inadvertently gain unauthorized access to meetings held in MS Teams. External guests can only attend a Teams meeting when they receive and accept an invitation from a DOI official through their non-DOI email address. Meeting organizers are responsible for ensuring meeting invitations are only shared for authorized purposes, and that all expected non-DOI participant information is accurate. External guests will remain in the Teams lobby until the meeting organizer or a participant in the meeting grants them access. External guests will receive notice to wait to be granted access to the meeting.

There is a risk that data may still be stored or available on previous vendor equipment such as servers and other storage devices after migration from BisonConnect Google Application for Government to Microsoft Cloud Computing Microsoft O365. A formal decommissioning process will be followed to certify removal of data. Additionally, all DOI data currently stored on the Google infrastructure is encrypted and data destruction policies in place per the FedRAMP package.

There is a risk the individuals participating in a MS Teams or Skype meeting may unknowingly be recorded without their consent. Teams and Skype are a part of O365 FedRAMP package and must adhere to compliance and industry standard framework for privacy and security which includes General Privacy and Security Terms of the Online Services Terms for data in the cloud. Meeting organizers are responsible for notifying participants on the intention to record meetings, and give individuals an option to decline being recorded prior to starting the meeting. Meeting organizers must also ensure discussions and chats are devoid of sensitive PII in nature and context. When a meeting recording is initiated in MS Teams to capture audio, video, or screen sharing, participants on the call are notified that a recording has started. A Privacy policy is displayed on the screen for individuals to review. The meeting notification is also posted to the chat history. MS Teams does not allow multiple recordings of the same meeting at the same time. Participants have the option of exiting, or may consent to the recording by participating in the meeting. All participants will be able to start and stop recording with the exception of guests external to DOI. Recording will continue even if the person who initiated the recording leaves the meeting, and will automatically stop when all participants leave the meeting. Recording will automatically stop after four hours. Additionally, Skype and Teams users can disable their cameras and microphones during calls.

There is also an option to use Teams Live, an extension of Teams for large audience meetings, and events. Teams Live gives event organizers control over attendee permissions, and meeting invitations.

There is a risk individuals may take screenshots during a Teams video call and screenshare activities without notifying participants or the individual sharing their computer screen. Individuals may upload photos as a background image for Team meetings that contain personal information. Individuals must ensure personal photos or images uploaded to their DOI GFE complies with Departmental and Federal policies.

There is a risk that meeting recordings may be shared outside meeting attendee group or the Department. Meeting recordings are stored on SharePoint Online or in Microsoft Stream for the recorder owner of the recording. The owner of the recording is responsible for ensuring proper access controls are in place such as to view, download, and delete permissions or sharing outside meeting participants including non-DOI guest attendees in Microsoft Stream. All DOI participants who were on the recorded call can visit their meeting chat history in Teams to play the recording. Still frame from a video recording will be visible to individuals when the link is shared with them. The owner of a recording can also edit the closed caption transcript in Microsoft Stream.

Additional O365 BisonConnect privacy protection measures include issuing security alerts to O365 BisonConnect account holders during times of heightened security threat. For example, when a targeted phishing campaign against O365 BisonConnect is detected, account holders may be provided with tips and techniques to prevent/reduce privacy compromise along with POC contact information for the local help desk, bureau security team, and DOI-CIRC team in case any response/recovery actions are needed.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

☒ Yes: *Explanation*

The O365 BisonConnect system is the unified messaging system for DOI and will contain all official DOI email communications. Information required for O365 is relevant to the purpose of the system. Data gathered within the MS Teams and Skype for Business Online application are contact information, and are used for the communication and collaboration among the DOI personnel to meet agency mission. Data stored within ODfB and SharePoint Online is consistent with the purpose of the service to promote collaboration.

☐ No

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

☒ No

O365 BisonConnect is intended to be an open, flexible, and full featured system for comprehensive messaging, information sharing and collaborative work. The system is not intended to derive new data or create previously unavailable data about an individual through aggregation from the information collected or communications exchanged. However, due to the integrated nature of O365 BisonConnect applications and the flexibility for O365 BisonConnect users to enter a wide variety of data, it is possible that new data could be created through aggregation of information about individuals.

C. Will the new data be placed in the individual's record?

☒ Yes: *Explanation*

O365 BisonConnect is not intended to derive new data or create previously unavailable data about an individual through data aggregation. However, due to the integrated nature of O365 BisonConnect applications and the flexibility for O365 BisonConnect users to enter a wide variety of data, it is possible that new data could be created that will be contained in one or more of O365 BisonConnect applications, such as Mail, Drive, and Calendar. In some instances, new data concerning an individual may be created as a result of an investigation or notification from a DOI network security system. While this new data will not be retained in O365 BisonConnect, it may be added to an individual's record in another DOI system.

☐ No

D. Can the system make determinations about individuals that would not be possible without the new data?

☐ Yes: *Explanation*

☒ No

O365 BisonConnect is not intended to derive new data or create previously unavailable data about individuals through aggregation from the information collected. Due to the integrated nature of O365 BisonConnect applications and the flexibility for O365 BisonConnect users to enter a wide variety of data, it may be possible for determinations to be made about individuals using any new data; however, the system is a communications and collaboration tool and is not intended to make determinations regarding individuals.

E. How will the new data be verified for relevance and accuracy?

As discussed above, O365 BisonConnect is not expected to derive or create new data. However, any new data that may be created or derived within the O365 BisonConnect system will be verified for relevance and accuracy at the time it is collected and used by DOI officials and only for authorized purposes.

F. Are the data or the processes being consolidated?

☒ Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

O365 BisonConnect is an integrated system that consolidates data from a number of existing systems, including Departmental email accounts previously held in multiple databases, as well as other applications in the suite of tools. In addition, data that is currently held in a variety of different locations, including Microsoft SharePoint and DOI file servers, may be transitioned by users to O365 BisonConnect. O365 BisonConnect applications have settings that restrict access to data created or entered by users. For example, users can use private settings for Sites and Drive files so content can be viewed only by users granted specific access.

O365 BisonConnect uses a variety of operational and technical controls to restrict unauthorized access and use. While O365 BisonConnect is a cloud-based system, it utilizes a private cloud community, as opposed to a public cloud service delivery model. Use of a private cloud significantly decreases penetration threats and associated risks. In addition, O365 BisonConnect employs a variety of management, operational and technical security controls.

Administrative access to O365 BisonConnect is granted only to authorized personnel on an official need-to-know basis. Unique administrator identification and authentication, passwords, least privileges and audit logs are utilized to ensure appropriate permissions and access levels. In addition, all administrative personnel, including contractors, must consent to rules of behavior and take annual end-user security awareness training, computer security role-based training, privacy awareness training, and role-based privacy training, and records training in order to obtain and maintain O365 BisonConnect administrator access.

☒ Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

O365 BisonConnect consolidates processes from a number of existing systems, including existing Departmental email systems, as well as Microsoft SharePoint and DOI file servers. O365 BisonConnect uses a variety of operational and technical controls to restrict unauthorized access and use. While O365 BisonConnect is a cloud-based system, it utilizes a private cloud community, as opposed to a public cloud service delivery model. Use of a private cloud significantly decreases penetration threats and associated risks. In addition, O365 BisonConnect employs a variety of management, operational and technical security controls.

Administrative access to O365 BisonConnect is granted only to authorized personnel on an official need–to-know basis. Unique administrator identification and authentication, passwords, least privileges and audit logs are utilized to ensure appropriate permissions and access levels. In addition, all administrative personnel, including contractors, must consent to rules of behavior and take annual end-user security awareness training, computer security role-based training, privacy awareness training, and role-based privacy training, and records training in order to obtain and maintain O365 BisonConnect administrator access.

☐ No, data or processes are not being consolidated.

G. Who will have access to data in the system or electronic collection? Indicate all that apply.

☒ Users
☒ Contractors
☒ Developers
☒ System Administrator
☐ Other: *Describe*

H. How is user access to data determined? Will users have access to all data or will access be restricted?

Access is controlled through user account management and authentication with DOI's AD system. Only authorized DOI personnel, contractors and volunteers will have access to the system, and that access is based on least privileges to perform job duties. Users and administrators can grant access to other information based on mission need. By default, all users only have access to information that they create or add. DOI performs regular audits of the system access and user interactions within the system.

ODfB and SharePoint Online have access control mechanisms that isolate data and have the capability to provide access to specified groups or individuals. Users manage these access controls to grant permissions and limit sharing of their documents to an individual user or a group; use of an application does not alter access permissions.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

☒ Yes. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*

Privacy clauses were included in the O365 service contract.

☐ No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

☐ Yes. *Explanation*

☒ No

K. Will this system provide the capability to identify, locate and monitor individuals?

☒ Yes. *Explanation*

O365 BisonConnect is integrated with the Symantec Vontu Data Loss Prevention (Symantec DLP) software. Symantec DLP monitors internet email and chat traffic to protect against the external transmission of sensitive data, including information concerning individuals such as social security numbers. Symantec DLP monitors data only; it cannot be set up to monitor individuals. O365 BisonConnect maintains a minimal ability to monitor administrator access and actions through administrator audit logs. The logs contain administrator name and a list of administrative actions taken, such as records changes or activation or deactivation of system features. O365 has an audit trail capability that can monitor user access and actions within the system.

☐ No

L. What kinds of information are collected as a function of the monitoring of individuals?

O365 BisonConnect is not intended to be used to monitor individuals. SharePoint Online and ODfB provide audit capabilities on addition, modification, or deletion of data within the systems. This information is only available to administrative personnel. Administrator reviews of audit logs will also help prevent any unauthorized monitoring or user behaviors. Through the auditing process username, IP address, time/date and login status are gathered to support user access controls, troubleshooting and incident response support.

M. What controls will be used to prevent unauthorized monitoring?

Access to administrative functions is strictly controlled and can only be granted by O365 BisonConnect administrators. Users must be included in security groups assigned to a O365 BisonConnect resource in order to access that particular resource. Users must obtain authorization from administrators with administrative rights delegated by the data owner and/or system managers to access resources within the environment. The users of the service are required to adhere to the system rules of behavior regarding the types of information that should not be stored in the O365 BisonConnect sub-systems or applications. Administrator reviews of audit logs will also help prevent any unauthorized monitoring or user behaviors.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

☒ Security Guards
☒ Key Guards
☒ Locked File Cabinets
☒ Secured Facility
☒ Closed Circuit Television
☐ Cipher Locks
☒ Identification Badges
☐ Safes
☐ Combination Locks
☒ Locked Offices
☐ Other. *Describe*

(2) Technical Controls. Indicate all that apply.

☒ Password
☒ Firewall
☒ Encryption
☒ User Identification
☒ Biometrics
☒ Intrusion Detection System (IDS)
☒Virtual Private Network (VPN)
☒ Public Key Infrastructure (PKI) Certificates
☒ Personal Identity Verification (PIV) Card
☐ Other. *Describe*

(3) Administrative Controls. Indicate all that apply.

☒ Periodic Security Audits
☒ Backups Secured Off-site
☒ Rules of Behavior
☒ Role-Based Training
☒ Regular Monitoring of Users' Security Practices
☒ Methods to Ensure Only Authorized Personnel Have Access to PII
☒ Encryption of Backups Containing Sensitive Data
☒ Mandatory Security, Privacy and Records Management Training
☐ Other. *Describe*

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

The Chief, End User Services Branch, Office of the Chief Information serves as the O365 Information System Owner and the official responsible for oversight and management of security controls and the protection of agency information processed and stored in O365. Each bureau/office program and user utilizing these O365 services are responsible for ensuring the security of data maintained in O365, and for meeting privacy and security requirements within their organization. The Information System Owner and Information System Security Officer are responsible for addressing privacy rights and complaints, and ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored in O365, in consultation with DOI privacy officials.

P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

The O365 Information System Owner is responsible for daily operational oversight and management of the system's security and privacy controls, for ensuring to the greatest possible extent that the data is properly managed and that all access to the data has been granted in a secure and auditable manner. The O365 Information System Owner and Information System Security Officer are responsible for ensuring that any loss, compromise, unauthorized access or disclosure of PII is reported to DOI-CIRC, DOI's incident reporting portal, and appropriate DOI officials in accordance with DOI policy and established procedures. Each bureau/office program and user utilizing these O365 services are responsible for ensuring the security of data maintained in O365, and for meeting privacy and security requirements within their organization and immediately reporting any potential compromise of data in accordance with Federal and DOI privacy breach response policy.